UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/822,927	04/12/2004	Eliot Lear	50325-0864	4441

29989 7590 03/27/2008

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
JOHNSON, CARLTON	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
03/27/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/822,927	LEAR, ELIOT	
	Examiner	Art Unit	
	CARLTON V. JOHNSON	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 December 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-21,23-25,27-29 and 31-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-21,23-25,27-29 and 31-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the Pre-Appeal Brief Request filed on 12/14/2007, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

2. This action is responding to application papers filed on **4-12-2004**. Claims **1, 3 - 21, 23 - 25, 27 - 29, 31 - 47** are pending. Claims **2, 22, 26, 30** have been cancelled. Claims **1, 8, 18, 21, 25, 29** are independent.

Response to Arguments

3. Applicant's arguments filed 12/14/2007 have been fully considered but they are moot due to new grounds of rejection.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. The claimed invention is directed to non-statutory subject matter. Claims **21, 23, 24, 34 - 37** are directed to a computer-readable medium based on non-statutory subject matter. The specification discloses a computer readable medium used to carry instructions that can be a transmission media using acoustic waves such as radio wave communications. Specification in paragraphs [0081] and [0082] states: "Transmission media can also take the form of acoustic waves, such as those generated during radio wave and infrared data communications." And the "computer readable media may be

involved in carrying one or more sequences of one or more instructions to processor 504 for execution". This claim is directed toward non-statutory subject matter such as radio wave communications as a type of computer readable medium. Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims **1, 21, 25, 29** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicant has failed to show how "verifying that two or more digital signatures, from the one or more digital signatures". There is no indication how two or more of an entity can come from one or more of an entity. If the entering selection is chosen from one (from one or more) then how can two (from two or more) be derived as claim limitation currently states.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims **1, 3 - 21, 23 - 25, 27 - 29, 31 - 47** are rejected under 35 U.S.C. 103 (a) as

being unpatentable over **Bosler et al.** (US Patent No. **20050010757**) in view of **Kinnis et al.** (US Patent No. **6,959,382**).

Regarding Claims 1, 21, 25, Bosler discloses a method, comprising the computer implemented steps of:

a) receiving trust information defining one or more trusted signatories; (see Bosler paragraph [0058], lines 5-7: public/private key pairs; paragraph [0060], lines 1-6: CAs (i.e. trusted signatories) distributing or granting certificates, received by user)

b) receiving configuration information comprising a hostname, one or more configuration directives for a host network element associated with the hostname, and one or more digital signatures of the hostname and configuration directives; (see Bosler paragraph [0058], lines 5-14: management (i.e. configuration) information transferred between manager and client, digital signature verification required)

c) attempting to verify the one or more digital signatures based on the trust information; (see Bosler paragraph [0008], lines 7-13: verification digital signature based on certificates received from CA (i.e. trust information))

e) applying the configuration directives to the host network element only when the one of more digital signatures are verified successfully. (see Bosler paragraph [0057], lines 29-33: utilize directives or commands after digital signature verification)

Bosler discloses wherein verifying that one or more digital signatures, from the one or more digital signatures, are valid and that two or more principals respectively associated with the two or more digital signatures have collective authority to perform the configuration directives on the host network element; (see Bosler paragraph [0008], lines 7-13; paragraph [0078], lines 7-15: management information, verify digital signature)

However, Kinnis discloses:

d) verifying that two or more digital signatures, from the one or more digital signatures, are valid. (see Kinnis col. 3, lines 3-24: first, second digital signatures for content, any number of signatures may be added; col. 3, lines 28-30: used for authentication purposes; col. 4, lines 25-27: content of any type can be protected with digital signature; col. 4, lines 31-34: certificate from Certificate Authority (CA))

It would have been obvious to one of ordinary skill in the art to modify Bosler to utilize multiple digital signatures as taught by Kinnis. One of ordinary skill in the art would have been motivated to employ the teachings of Kinnis in order to obtain certificates, keys, and generate digital signatures that may be stored independent of other tools. (see Kinnis col. 2, lines 20-26: " ... *Accordingly, it is desirable to provide a means to generate digital signatures that are not specific to an application, such as an email client. The digital signature service also provides the functionality to obtain certificates, manage private--public keys, and generate digital signatures for documents that may be stored independent of other tools used by the user.* ... ")

Regarding Claims 3, 4, Bosler discloses a method as recited in Claim 1, further comprising the steps of

a) receiving in association with a particular configuration directive, security information defining a number of required signatures and required principals; (see Bosler paragraph [0058], lines 21-28: receive security information with directive (i.e. command, management message))

b) applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals and only upon successively validating all required signatures. (see Bosler paragraph [0058], lines 5-14: digital signature authentication; paragraph [0069], lines 1-5: apply directives or commands after authentication)

Regarding Claims 5, 15, Bosler discloses a, and wherein public keys for the digital signatures are stored on the host. (see Bosler paragraph [0073], lines 4-7: security information stored in central location (i.e. host system), (i.e. option, each individual system or host))

Regarding Claims 6, 16, Bosler discloses a method as recited in Claim 1, wherein the digital signatures use public key cryptography, wherein public keys for the digital signatures are stored on a key server and retrieved from the key server as part of attempting to validate the digital signatures. (see Bosler paragraph [0007], lines 6-8:

public key cryptography authentication; paragraph [0073], lines 4-7; paragraph [0060], lines 1-6: security information stored in central location or in each individual system or host, certification server (i.e. key server))

Regarding Claims 7, 17, Bosler discloses a method as recited in Claim 1, wherein the digital signatures use public key cryptography, and wherein public keys for the digital signatures received in a digital certificate and extracted from the digital certificate as part of attempting to validate the digital signatures. (see Bosler paragraph [0058], lines 5-7: public/private key pair; paragraph [0060], lines 1-6: Certificate Authority (CA) , public key certificate; paragraph [0008], lines 7-13: verification (i.e. validation) with digital signature)

Regarding Claims 8, 18, Bosler discloses a method, comprising the computer implemented steps of:

a) receiving a public key for a user of the network devices; receiving trust information defining one or more trusted signatories; (see Bosler paragraph [0058], lines 5-7: public/private key pairs; paragraph [0060], lines 1-6: CAs (i.e. trusted signatories) distributing or granting certificates)

b) receiving configuration control information that includes a time period during which a valid digital signature is required for applying one or more particular configuration directives; (see Bosler paragraph [0071], lines 1-13; paragraph [0073], lines 77-22: time-based certificate, directive authentication)

c) receiving configuration information comprising a hostname, one or more configuration directives for a host network element associated with the hostname, one or more digital signatures of the hostname and configuration directives, and a date time value; (see Bosler paragraph [0058], lines 5-14: management (i.e. configuration) information transferred between manager and client, digital signature verification required)

d) determining if the date time value is within the time period; (see Bosler paragraph [0073], lines 17-22: time based verification for certificate, time period valid)

e) determining if the one or more configuration directives have been previously received during the time period; (see Bosler paragraph [0069], lines 1-5: process configuration directive(s), commands) and

f) only when the date time value is within the time period (see Bosler paragraph [0073], lines 17-22: time based certificate) and the one or more configuration directives have not been previously received during the time period, attempting to verify the one or more digital signatures based on the trust information, and applying the configuration directives to a network element only when the one or more digital signatures are verified successfully. (see Bosler paragraph [0058], lines 5-14: apply directives when digital signature authenticated)

Regarding Claims 9, 10, Bosler discloses a method as recited in Claim 8, wherein the step of determining if the one or more configuration directives have been previously received during the time period comprises the steps of

a) generating a secure hash of the one or more configuration directives; (see Bosler paragraph [0078], lines 3-15: generate secure hash value for authentication)

b) determining if the secure hash is found in non volatile memory. (see Bosler paragraph [0078], lines 3-15; paragraph [0067], lines 4-8: memory, workspace for data processing: memory (i.e. non-volatile))

Regarding Claim 11, Bosler discloses a method as recited in Claim 8, further comprising the step of storing the secure hash in non volatile memory, in association with an expiration value, when the date time value is within the time period and the one or more configuration directives have not been previously received during the time period. (see Bosler paragraph [0067], lines 4-8: memory, workspace for data processing; paragraph [0071], lines 1-13; paragraph [0073], lines 4-7: time-based certificates; paragraph [0078], lines 3-15: hash (i.e. digest) values utilized for authentication)

Regarding Claim 12, Bosler discloses a method as recited in Claim 8, further comprising the steps of verifying that the one or more digital signatures is valid and that one or more principals respectively associated with the digital signatures have collective authority to perform the directives on the host. (see Bosler paragraph [0058], lines 5-14: mutual authentication required before directive(s) or command(s) implemented)

Regarding Claims 13, 14, Bosler discloses a method as recited in Claim 8, further

comprising the steps of

a) receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals; (see Bosler paragraph [0058], lines 21-28: key, security information received with directive or command)

b) applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals and only upon successively validating all required signatures. (see Bosler paragraph [0058], lines 5-14; paragraph [0069], lines 1-5: validate digital signature, process directive or command)

Regarding Claim 18, Bosler discloses a method for verifying configuration changes for network devices using digital signatures, comprising the computer implemented steps of:

a) receiving a public key for a user of the network devices; (see Bosler paragraph [0058], lines 5-7: public/private key pairs; paragraph [0060], lines 1-6: CAs (i.e. trusted signatories) distributing or granting certificates (i.e. public key certificate), received by user)

b) receiving configuration control information that includes a time period during which a valid digital signature is required for applying one or more particular configuration directives to a specified network device; (see Bosler paragraph [0071], lines 1-13; paragraph [0073], lines 17-22: time based certificate)

c) receiving configuration information comprising a hostname, one or more configuration directives for the specified network device associated with the hostname, one or more digital signatures of the hostname and configuration directives, and a date time value; (see Bosler paragraph [0058], lines 5-14: management (i.e. configuration) information transferred between manager and client, digital signature verification required)

d) determining if the date time value is within the time period; (see Bosler paragraph [0073], lines 17-22: time based certificate, time period valid)

e) determining if the one or more configuration directives have been previously received during the time period, by generating a secure hash of the one or more configuration directives and determining if the secure hash is found in memory; (see Bosler paragraph [0078], lines 3-15: hash (i.e. digest) utilized) and

f) only when the date time value is within the time period and the one or more configuration directives have not been previously received during the time period, (see Bosler paragraph [0073], lines 17-22: time-based certificate, time period valid)

performing the steps of:

g) attempting to verify the one or more digital signatures based on generating a secure hash of the one or more configuration directives using the public key and comparing the secure hash to the one or more digital signatures, and applying the configuration directives to a network element only when the one or more digital signatures are verified successfully. (see Bosler paragraph [0078], lines 3-

15: hash generation, authentication)

Regarding Claims 19, 23, 31, Bosler discloses a method as recited in any of Claims 1, 8, or 18, wherein the one or more digital signatures comprise a first digital signature of the one or more configuration directives by a first user, and a second digital signature by a second user, wherein the second digital signature is applied to a resultant of the first digital signature. (see Bosler paragraph [0078], lines 7-15: comparison (i.e. is applied) of resultant hashes (i.e. digest, digital signature) for authentication)

Regarding Claims 20, 24, 32, Bosler discloses a method as recited in any of Claims 1, 8, or 18, wherein the one or more digital signatures comprise a first digital signature of a first portion of the one or more configuration directives by a first user, a second digital signature of a second portion of the one or more configuration directives by a second user, and a third digital signature by a third user, wherein the third digital signature is applied to a resultant of the first digital signature and the second digital signature. (see Bosler paragraph [0078], lines 7-15: comparison (i.e. is applied) of resultant hashes (i.e. digest, digital signature) for authentication)

Regarding Claim 27, Bosler discloses an apparatus as recited in Claim 25, wherein the one or more digital signatures comprise a first digital signature of the one or more configuration directives by a first user, and a second digital signature by a second user, wherein the second digital signature is applied to a resultant of the first digital signature.

(see Bosler paragraph [0078], lines 7-15: comparison (i.e. is applied) of resultant hashes (i.e. digest, digital signature) for authentication)

Regarding Claim 28, Bosler discloses an apparatus as recited in Claim 25, wherein the one or more digital signatures comprise a first digital signature of a first portion of the one or more configuration directives by a first user, a second digital signature of a second portion of the one or more configuration directives by a second user, and a third digital signature by a third user, wherein the third digital signature is applied to a resultant of the first digital signature and the second digital signature. (see Bosler paragraph [0078], lines 7-15: comparison (i.e. is applied) of resultant hashes (i.e. digest, digital signature) for authentication)

Regarding Claim 29, Bosler discloses An apparatus for verifying configuration changes for network devices using digital signatures, comprising: a network interface that is coupled to the data network for receiving one or more packet flows therefrom;

a) a processor; (see Bosler paragraph [0067], lines 4-8: processor)

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

b) receiving trust information defining one or more trusted signatories; (see Bosler paragraph [0058], lines 5-7: public/private key pairs; paragraph [0060], lines 1-6: CAs (i.e. trusted signatories) distributing or granting certificates, received by user)

c) receiving configuration information comprising a hostname, one or more configuration directives for a host network element associated with the hostname, and one or more digital signatures of the hostname and configuration directives; (see Bosler paragraph [0058], lines 5-14: management (i.e. configuration) information transferred between manager and client, digital signature verification required)

d) attempting to verify the one or more digital signatures based on the trust information; (see Bosler paragraph [0008], lines 7-13: verify digital signature)

e) verifying that two or more digital signatures, from the one or more digital signatures, are valid and that two or more principals respectively associated with the two or more digital signatures have collective authority to perform the configuration directives on the host network element; (see Bosler paragraph [0008], lines 7-13: verify digital signature)

f) applying the configuration directives to the home network element only when the one or more digital signatures are verified successfully. (see Bosler paragraph [0058], lines 5-14; paragraph [0069], lines 1-5: signature verification, process directive)

Bosler discloses wherein verifying that one or more digital signatures, from the one or more digital signatures, are valid and that two or more principals respectively associated with the two or more digital signatures have collective authority to perform the configuration directives on the host network element; (see Bosler paragraph [0008], lines 7-13; paragraph [0078], lines 7-15: management information,

verify digital signature)

However, Kinnis discloses:

e) verifying that two or more digital signatures, from the one or more digital signatures, are valid. (see Kinnis col. 3, lines 3-24: first, second digital signatures for content, any number of signatures may be added; col. 3, lines 28-30: used for authentication purposes; col. 4, lines 25-27: content of any type can be protected with digital signature; col. 4, lines 31-34: certificate from Certificate Authority (CA))

It would have been obvious to one of ordinary skill in the art to modify Bosler to enable the capability to utilize multiple digital signatures as taught by Kinnis. One of ordinary skill in the art would have been motivated to employ the teachings of Kinnis in order to obtain certificates, keys, and generate digital signatures that may be stored independent of other tools. (see Kinnis col. 2, lines 20-26)

Regarding Claims 33, 38, 43, Bosler discloses a computer-readable medium, apparatus as recited in Claims 21, 25, 29, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of: receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals (see Bosler paragraph [0058], lines 21-28: receive security information with directive (i.e. command, management message)); applying the particular configuration directive only when the configuration information has the number of required signatures by the required

principals. (see Bosler paragraph [0058], lines 5-14: digital signature authentication; paragraph [0069], lines 1-5: apply directives or commands after authentication; paragraph [0057], lines 23-28; paragraph [0066], lines 1-4: software, implementation means)

Regarding Claims 34, 39, 44, Bosler discloses a computer-readable medium, apparatus as recited in Claims 21, 25, 29, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of: receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals; applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals and only upon successively validating all required signatures. (see Bosler paragraph [0058], lines 5-7: public/private key pair; paragraph [0060], lines 1-6: Certificate Authority (CA) , public key certificate; paragraph [0008], lines 7-13; paragraph [0078], lines 7-15: verification (i.e. validation) with digital signature(s); paragraph [0057], lines 23-28; paragraph [0066], lines 1-4: software, implementation means)

Regarding Claims 35, 40, 45, Bosler discloses a computer-readable medium, apparatus as recited in Claims 21, 25, 29, wherein the digital signatures use public key cryptography, and wherein public keys for the digital signatures are stored on the host network element. (see Bosler paragraph [0073], lines 4-7: security information stored in

central location (i.e. host system), (i.e. option, each individual system or host); paragraph [0057], lines 23-28; paragraph [0066], lines 1-4: software, implementation means)

Regarding Claims 36, 41, 46, Bosler discloses a computer-readable medium, apparatus as recited in Claims 21, 25, 29, wherein the digital signatures use public key cryptography, wherein public keys for the digital signatures are stored on a key server and retrieved from the key server as part of attempting to validate the digital signatures. (see Bosler paragraph [0007], lines 6-8: public key cryptography authentication; paragraph [0073], lines 4-7; paragraph [0060], lines 1-6: security information stored in central location or in each individual system or host, certification server (i.e. key server); paragraph [0057], lines 23-28; paragraph [0066], lines 1-4: software, implementation means)

Regarding Claims 37, 42, 47, Bosler discloses a computer-readable medium as recited in Claims 21, 25, 29, wherein the digital signatures use public key cryptography, and wherein public keys for the digital signatures received in a digital certificate and extracted from the digital certificate as part of attempting to validate the digital signatures. (see Bosler paragraph [0058], lines 5-7: public/private key pair; paragraph [0060], lines 1-6: Certificate Authority (CA) , public key certificate; paragraph [0008], lines 7-13: verification (i.e. validation) with digital signature; paragraph [0057], lines 23-28; paragraph [0066], lines 1-4: software, implementation means)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carlton V. Johnson
Examiner
Art Unit 2136

CVJ
March 17, 2008

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136